Montage Health Consolidates Its Cybersecurity Strategy with CrowdStrike

When Tahir Ali became CTO and CISO at Montage Health in 2021, he inherited a unique set of cybersecurity challenges. For one, the healthcare sector was getting bombarded with attacks, including distributed denial of service (DDoS), phishing and social engineering attacks.

At the same time, the California-based nonprofit healthcare system was integrating more networked medical devices, employee-owned devices, AI applications and cloud services into its infrastructure. While these innovations brought operational efficiencies and a better patient experience, they also expanded the attack surface.

Against this backdrop, Ali performed a security assessment of his available tools and resources. What he found was a set of non-integrated, legacy security tools that struggled to detect and stop modern attacks. Furthermore, he didn't have the 24/7 coverage needed to defend against increasingly aggressive threat actors.

Ali began searching for a strategic partner to provide both a modern cybersecurity platform and 24/7 managed detection and response. That's when he found CrowdStrike.

Consolidating with CrowdStrike

The search for a strategic cybersecurity partner didn't take long. Ali compared four vendors and landed on CrowdStrike after a successful proof of concept (POC).

"One big consideration during the POC was agent performance. We run a lot of virtual desktop infrastructure (VDI), so we didn't want our endpoint agent slowing down login or boot-up times," explained Ali. "CrowdStrike was the superstar of the POC, so we bought it."

Montage Health quickly deployed the lightweight CrowdStrike Falcon® agent to its 5,000+ endpoints, replacing its legacy security software with the AI-native Falcon platform. The modular architecture of the Falcon platform enabled the healthcare system to start with CrowdStrike Falcon® Insight XDR for extended detection and response, then easily add new protections using the same agent and command console.

"Our push was to get to a full security platform from a single vendor, but I wasn't willing to sell my soul for it," explained Ali. "Because our CrowdStrike XDR deployment was so successful, we had confidence to move forward with additional Falcon platform modules."

Montage Health soon deployed CrowdStrike Falcon® Identity Protection, CrowdStrike Falcon® Discover for IT hygiene, CrowdStrike Falcon® Prevent next-gen antivirus and CrowdStrike Falcon® Adversary Intelligence. This suite of innovative solutions gave Montage Health industry-leading protection across critical attack surfaces, plus many other benefits of cybersecurity consolidation, including increased speed, and lower cost and complexity.

MONTAGE Health

INDUSTRY

Healthcare

LOCATION/HQ

California, USA

CHALLENGES

- Cyberattacks on the healthcare sector were getting more frequent and sophisticated.
- Montage Health's attack surface was growing due to an influx of networked medical devices, employee-owned devices, AI applications and cloud services.
- The company's previous set of non-integrated, legacy security tools struggled to detect and stop modern attacks.

SOLUTION

Montage Health licensed the CrowdStrike Falcon® XDR platform along with several product modules and services, including CrowdStrike Falcon® Insight XDR for extended detection and response, CrowdStrike Falcon® LogScale and CrowdStrike Falcon® Complete for 24/7 managed detection and response.

RESULTS

- Zero breaches with CrowdStrike
- 24/7 managed detection and response
- 5x fewer security events requiring Montage Health to investigate
- 53 seconds: the average time it takes Montage Health to triage an event

Next-Gen SIEM for Unmatched Speed and Scale

In 2021, Montage Health became an early adopter of CrowdStrike Falcon® LogScale for next-gen SIEM and log management. Built for the speed and scalability requirements of the modern SOC, Falcon LogScale offers real-time alerting, fast search and world-class threat intelligence for up to 80% less cost than legacy log management solutions.

"It used to take us weeks to investigate an incident. Now it takes us 25 minutes and we know exactly what happened. Queries are faster too … it's maybe a gazillion times faster," joked Ali.

Falcon LogScale is built on a unique, index-free architecture that delivers security logging at petabyte scale. Montage Health started with a small instance of Falcon LogScale and was able to easily scale up once it saw what the solution could do.

"Before Falcon LogScale, it would take us 3 to 4 months to scale our log management capabilities, including all the servers, storage, monitoring and backup needed to grow a few hundred terabytes. With LogScale, we can add 300 to 400 terabytes of additional scalability in days," said Ali. "From my perspective, LogScale is faster than any other product out there."

With 20 years of experience in IT and security, Ali has used a number of SIEM and log management solutions throughout his career. For him, Falcon LogScale delivers the optimal mix of performance and interoperability.

"Falcon LogScale gives us total visibility of our environment. Compared to other SIEMs I've used, LogScale performs better, is more customizable and requires less overhead," said Ali. "When we switched to LogScale, the difference was obvious. Plus, it integrates seamlessly with the Falcon platform, which made it that much more attractive to us."

Better Security by the Numbers

For Montage Health, having innovative cybersecurity technology is only half the battle. The company also relies on CrowdStrike Falcon® Complete for 24/7 managed detection and response. With Falcon Complete, Montage Health gets both around-the-clock protection and the expertise needed to stop even the most sophisticated cyberattacks.

All told, the combination of the Falcon platform and Falcon Complete has revolutionized the culture of security at Montage Health, allowing the nonprofit to deliver the same high level of excellence in security as it does in the clinical setting.

The data bears this out: Monthly investigations have dropped from 102 to 56. Monthly events requiring Montage Health to investigate have dropped from 11 to 2. And the time required to investigate and triage each event dropped from several hours to only 53 seconds.

"I know it sounds crazy but it's all true," concluded Ali. "We're very happy with CrowdStrike."

"From my perspective, LogScale is faster than any other product out there."

Tahir Ali, CTO and CISO,
Montage Health

CROWDSTRIKE PRODUCTS

- Falcon Insight XDR for extended detection and response
- Falcon LogScale next-gen SIEM
- Falcon Identity Protection
- Falcon Firewall Management
- Falcon Discover for IT hygiene
- Falcon Prevent next-gen antivirus
- Falcon Adversary OverWatch™ managed threat hunting
- Falcon Complete for 24/7 managed detection and response
- Falcon Adversary Intelligence

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more **www.crowdstrike.com**